requirement, and as failing to comply with the written description requirement, and were rejected under 35 U.S.C. 112, second paragraph, as being vague and indefinite. Claims 1-13 were further rejected under 35 U.S.C. 102(e) as anticipated by U.S. Patent 6, 678,835, Shah, et al., *State transition protocol for high availability units,* having a priority date of June 10, 1999 (henceforth "Shah"). Applicants are traversing the rejections.

Remarks

The rejections of claims 8 and 10 under 35 U.S.C. 112

These rejections are discussed in the order in which they are made in the Office action of 4/5/05. All of these rejections appear to be rooted in Examiner's difficulties with the language "determining that the particular entity *may not* perform the given action if the further condition is not satisfied at the time the processor responds to the request" of claim 108 and the language "determining that the requesting entity *may not* perform the action unless the particular manner is the manner specified by the action attribute" of claim 109. In both claim 108 and 110, "may not" is used in the sense of "is not permitted to", as in the English sentence, "A sentry may not leave his post."

The "best mode" rejection

The "best mode" requirement of 35 U.S.C. 112, first paragraph, applies to the Specification, rather than the claims, and thus cannot form the basis for a rejection of claims 8 and 10. More particularly, as should be apparent from the discussion of how "may not" is used above, the use of "may not" in claims 108 and 110 conceals nothing.

The "enablement" rejection

The "enablement" requirement of 35 U.S.C. 112, first paragraph, also applies to the Specification, rather than the claims, and thus cannot form the basis for a rejection of claims 8 and 10. With regard to amended claims, the issue is whether the claims as amended are supported by the Specification as originally filed. In the instant case, if Examiner understands that "may not" is being used in the sense of "is not permitted to",

Examiner will see that the claims are fully supported at least at page 85, line 1 through 87, line 16 of the disclosure, with implementation details being described beginning at page 87, line 19.

The "negative limitation" rejection

It should by now be clear that "may not" as used in claims 8 and 10 is not a "negative limitation" on the order of "the shaft is not square". Further , as pointed out with regard to the "enablement" rejection, claims 8 and 10 are fully supported by the Specification as originally filed.

The rejection under 35 U.S.C. 112, second paragraph

As pointed out above, "may not" as used in claims 8 and 10 is neither vague nor indefinite.

The rejection of claims 1-13 as anticipated by Shah

The problem with this rejection is that Shah is not available as a reference against the present patent application. As pointed out in the *Cross Reference to Related Patent Applications* of the present patent application, the PCT application of which the present application is the U.S. national phase claims priority from U.S. Provisional Patent Application 60/091,130, Hannel, et al., *Generalized Policy Server*, filed 6/29/98, while Shah's earliest priority date is 6/10/99. Provisional patent application 60/091,130 should be included in the present patent application's file wrapper, but in case it is not, Applicants are including the most relevant portion of the provisional patent application with this response, so that Examiner can see that the claims are fully supported by the provisional patent application as filed.

Conclusion

Applicants have traversed the rejections under 37 C.F.R. 112 and the rejections under 35 U.S.C. 102 and have thereby been fully responsive to Examiner's Office action of 10/25/04, as required by 37 C.F.R. 1.111(b). Applicants have thereby satisfied the requirements of 37 C.F.R. 1.111(b) and respectfully request that Examiner continue with

his examination, as provided by 37 C.F.R. 1.111(a). A Petition for a one-month extension of time under 37 C.F.R. 1.136 is attached along with a check for $120.00 Please charge any additional fees required for this response or refund any overpayment to deposit account number 501315.

Respectfully submitted,

Gordon E. Nelson

Attorney of record,
Gordon E. Nelson
57 Central St., P.O. Box 782
Rowley, MA, 01969,
Registration number 30,093
Voice: (978) 948-7632
Fax: (617) 788-0932

August 3, 2005
Date

Certificate of Mailing

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to:

Commissioner for Patents
Alexandria, VA 22313-1450

on 8/3/2005
(Date)
Gordon E. Nelson, #30,093

Gordon E. Nelson
(Signature)

GENERALIZED POLICY SERVER

A system for making decisions about the conditions under which an action may be taken on a resource.

Conclave Technology

Cliff Hannel

Internet Dynamics, Inc.

June 28, 1998

Summary

This paper describes the generalization of the policy server technology contained within Internet Dynamics' product, Conclave. This generalization extends the ability of the product to manage policies and provide decisions about the actions that entities may perform on resources and the constraints those actions may be subject to.

An important feature of this technology is that it allows those responsible for managing disparate resources (Policymakers) to centrally manage policies in an abstract, meaningful and concise way. By adding a method (protocol) for remotely requesting policy decisions (Evaluation Requests) from the server, a wide range of devices and applications can be used to enforce a set of centrally defined policies.

The Policy Server consists of the following principal elements:

- The policy database(s)
- The policy management user interface
- The Evaluation Engine (including Entity and Resource classification)
- The protocol for servicing Evaluation Requests

The Policy Server should be considered separate and distinct from the device or application that services or intercepts resource requests and enforces policies (the Enforçement Device).

Current Implementation and Future Scenarios

This document describes both the current implementation of the described technology within Conclave and the future anticipated use of a generalized, distributed product based on the same technology. Currently, Conclave combines both Policy Server and Enforcement Device functionality as they pertain to controlling access to IP-based network resources. In the future, with the full generalization of the Policy Server technology described in this document, the same administrative interface, database and evaluation engine could be used for management of resources unrelated to those currently being controlled.

Policy Syntax

Each Policy is of the form:

Entity [is | are] [allowed to | denied] *Action* [to | to the] *Resource* [from | on | during] *TimeInterval(s)* [with | when] *ActionAttribute(s)*

The following are examples of policy statements:

- 'Employees' are allowed to 'Access' the 'HR web site'
- 'Engineering' is allowed to 'Access' the 'Engineering File Server' from '9:00 am - 5:00 pm weekdays' with 'encryption=RC4-40, tunnel server = 192.168.36.5'
- 'Marketing' is allowed to 'print to' the 'Marketing Printer' with 'type=color'
- 'Everyone' is denied 'Access' to 'Non-business Web Sites'

- 'Everyone' is allowed to 'Access' the 'World Wide Web' from '9:00am to 5:00pm Monday-Friday' with 'bandwidth=50%'
- 'Secretaries' are allowed to 'fax to' the 'corporate fax server' with 'price=.25'

The Policy Server manages and evaluates a collection of policies. The purpose of creating a collection of policies is to model a 'real world' environment where any number of Entities may be attempting to perform Actions on any number of Resources. In order for such a system to be useful, it must reduce overall complexity by shielding the policymaker from the minute details of each resource request. It must also provide a means of building a model that closely mimics the policymakers' way of thinking about their environment.

Since the Enforcement Device may provide arbitrary information about the requesting Entity, Action and Resource as part of an Evaluation Request, the Policy Server can be extended to manage Entity, Action and Resource types not known in advance.

Each part of the policy statement is described in more detail below.

Entity Definition

The Entity within a Policy refers to the requestor of a Resource. Within the Policy Server database, Entities (also referred to as Users) are grouped according to attributes that are provided as part of an Evaluation Request or discovered by the Policy Server. This discovery process allows the Policy Server to act as an 'authentication broker' on behalf of the Enforcement Device, which does not need to support each authentication method itself. Conversely, the Enforcement Device might provide authentication information not discoverable by the Policy Server as part of an Evaluation Request.

An Entity may belong to any number of named groups, and groups may also belong to any number of other groups. This allows familiar naming and an arbitrary hierarchy to be established to model the user community in the way that most closely mimics the environment.

The Conclave Policy Server currently supports the following methods for determining which groups an Entity is a member of:

- x.509 certificate: group membership may be obtained if information within the Entity's certificate matches a pattern established by the Policymaker.
- Challenge-Response (Token) Authentication (various types): group membership may be obtained by successfully responding to a challenge provided by an authentication server proving an association with a named user.
- Windows ID: group membership may be obtained if an entity is a member of a Domain or Domain Group based on their workstation login.
- IP Address and Domain Name: group membership may be obtained if the entity's address falls within a specified range or an inverse DNS lookup of that address matches a specified pattern.

Additional methods may be added in the future, and may include a means of adding methods supported by the Enforcement Device that are not known to the Policy Server in advance.

Action Definition

The *Action* specifies what operation the requestor would like to perform on the resource. The most common example of an Action is to *access* a resource. Each action may be either allowed or denied. In the absence of any explicit policy governing a particular action, a default policy is applied. Generally, this default policy is to deny the action.

Other examples of actions may be to administer, read, modify, create, print or send.

The Policy Server could allow additional Actions to be defined that were not known in advance.

Resource Definition

The *Resource* describes the controlled item that the requestor is attempting to perform the action on. Generally, the Resource being requested is provided by the Enforcement Device as part of the Evaluation Request.

When referring to network resources using Internet Protocol (IP), the resource is specified as a Server (by name or IP address), a Service (by port number or other means) and a service-specific resource (a web directory or page, for example). Other examples of resources may be a page to be printed to a color printer, a voice message from an Interactive Voice Response (IVR) system or page to be transmitted through a fax machine.

Resources may belong to any number of named Information Sets, which may in turn belong to any number of other Information Sets. This allows familiar naming and an arbitrary hierarchy to be established to model the available resources in a way that mimics the environment being controlled.

The Policy Server could allow additional Resource types to be defined that were not known in advance.

Time Interval Definition

The Time Interval Definition specifies when an action may be performed. The following are examples of Time Interval Definitions:

- 12:00 am - 8:00 am
- 8:00am - 5:00pm Monday - Friday except December 25
- Weekends
- January 1, 2000

Action Attribute Definition

The conditions under which an action may be taken can be described with any number of Action Attributes. The Action Attributes may be associated with the Entity, Resource or Policy.

Conclave currently supports the following Action Attributes:

- Encryption algorithm required
- Tunnel server to be used (for IPSEC)
- Authentication type required

Other examples of Action Attributes might include:

- Class of service (bandwidth allocation) to be applied
- Route or media type to be used
- Billing rate to be applied
- Maximum quantity for this transaction
- Maximum time allowed to complete transaction

The Policy Server could allow additional Action Attributes to be defined that were not known in advance.

Related Technologies Described Elsewhere

Conclave Policy Management: this describes the use of a distributed database and the delegation of administrative authority used in managing policies.

Adaptive Encryption and Authentication (SEND): this describes Conclave's means of dynamically determining the appropriate level of encryption to be applied when transmitting a resource to a given requestor.

(others TBD)